Notice of Allowability	Application No.	Applicant(s)	
	09/898,136	CHEN ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *examiner's amendment authorized on 4/27/06*.

2. ☒ The allowed claim(s) is/are *1-4*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Robert Marley on 4/26/07.

The application has been amended as follows:

- Replace paragraph [01] with the following amended paragraph:

[01] This application is a divisional application of U.S. patent application serial no. 09/898,136 filed July 3. 2001 entitled "SYSTEM FOR DENYING ACCESS TO CONTENT GENERATED BY A COMPROMISED OFF LINE ENCRYPTION DEVICE AND FOR CONVEYING CRYPTOGRAPHIC KEYS FROM MULTIPLE CONDITIONAL ACCESS SYSTEMS". This application is also related to U.S. Patent Application No. 08/420,710, now U.S. Patent No 5,627,892, entitled "DATA SECURITY SCHEME FOR POIT-TO-POINT COMMUNICATION SESSIONS," filed April 19, 1995, U.S. Patent Application No. 09/898,184, entitled "SYSTEM FOR SECURELY DELIVERNG PRE-ENCRYPTED CONTENT ON DEMAND WITH ACCESS-CONTROL," filed July 3, 2001; U.S. Application No. 09/898,168, entitled "SYSTEM FOR SECURING ENCRYPTION RENEWAL

DEVICE AND FOR REGISTRATION AND REMOTE ACTIVATION OF ENCRYPTION DEVICE," filed July 3, 2001.

- Replace paragraph [09] with the following amended paragraph:

[09] One solution to the aforementioned problem is disclosed in copending related application entitled, "SYSTEM FOR SECURELY DELIVERWG PRE-ENCRYPTED CONTENT ON DEMAND WITH ACCESS CONTROL," serial no. 09/898,184, filed July 3, 2001, which is hereby incorporated by reference in its entirety. In U.S. serial no. 09/898,184, a system is disclosed that encrypts content offline (typically before the content is requested by the user) before it is distributed to point-to-point systems such as cable systems. The system allows content to be encrypted once, at a centralized facility, and to be useable at different point-to-point systems. Advantageously, the pre-encrypted contents in the present invention have indefinite lifetimes. The system periodically performs an operation called ECM retrofitting, enabling the content to be useable in multiple systems and useable multiple times in the same system. The amount of data being processed during ECM retrofitting is very small (on the order of several thousand bytes). There is no need to reprocess the pre-encrypted contents. This is a significant advantage, as several thousand bytes represent only a

tiny fraction of the size of a typical 2-hour video program, which is about 3 gigabytes (3,000,000,000 bytes) in size.

- Replace paragraph [10] with the following amended paragraph:

[10] In a first embodiment, the system of U.S. serial no. 09/898,184, includes a content preparation system (CPS) for pre-encrypting the content offline to form pre- encrypted content; an encryption renewal system (ERS) for generating entitlement control messages (ECMs) that allow the pre-encrypted content to be decryptable for a designated duration; and a conditional access system (CAS). Conventionally, the CAS controls a population of set-top boxes using a randomly generated periodical key. Only with possession of the periodical key can the pre-encrypted content be decrypted by the set-top boxes. The periodical key is initially forwarded to the ERS which thereafter generates an ECM containing information regarding the periodical key.

- The claims have been amended as follows

1. (Currently Amended) A method for use in cable systems, the method for forwarding messages containing cryptographic keys from multiple conditional access systems that control a population of set-top boxes to an encryption renewal system, the method comprising:

defining a fictitious address for a single virtual set-top box, wherein said fictitious address is used by said multiple conditional access systems to address said encryption renewal system;

storing ~~a single~~ said fictitious address ~~of a virtual set-top box, said fictitious address being identical for~~ at each of said multiple conditional access systems;

generating a unique key within each of said multiple conditional access systems as a function of the identity of each particular multiple conditional access system;

encrypting said unique key for each of said multiple conditional access systems; ~~and~~

encapsulating each of said encrypted unique keys in an encoded message; and ~~encoded to be forwarded to said single fictitious address.~~

forwarding the encoded message to said fictitious address.

23-35. (Canceled)

2. The following is an examiner's statement of reasons for allowance. The present invention is directed to a method for forwarding messages containing cryptographic keys from multiple conditional access systems that control a population of set-top boxes to an encryption renewal system. More specifically, independent claim 1 identifies the uniquely distinct features: defining a fictitious address for a single virtual set-top box, wherein said fictitious address is used by said multiple conditional access systems to address said encryption renewal system. The closest prior art, Wasilewski et

al (6,157,719), teaches a conditional access system utilizing the service of multiple encryption renewal systems (Service Encryption and ECM Streamer SEES) wherein the conditional access system sends an EMM message containing a key to one of the SEESs (fig. 6; col. 15, lines 3-23). Another prior art, "EBU Technical Review No. 226 - Functional model of a conditional access system" by "EBU Project Group", teaches that different conditional access systems can share certain elements. However, Wasilewski and "EBU Project Group", either alone or in combination, does not teach the specific features mentioned above. The prior art, taken either singly or in combination, fails to anticipate or fairly suggest the limitations of applicant's independent claim, in such a manner that a rejection under 35 U.S.C 102 or 103 would be proper. The claimed invention is therefore considered to be in condition for allowance as being novel and nonobvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MD

Minh Dinh
Examiner
Art Unit 2132

4/26/07

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100